行列環の補完的部分環について (函数解析学による一般化エントロピーの新展開)

AUTHOR(S):

大野, 博道

CITATION:

大野, 博道. 行列環の補完的部分環について (函数解析学による一般化エントロピーの新展開). 数理解析研究所講究録 2013, 1852: 205-209

ISSUE DATE:

2013-09

URL:

http://hdl.handle.net/2433/195144

数理解析研究所講究録
第1852巻 2013年 205-209

行列環の補完的部分環について

信州大学工学部　大野 博道
Department of Mathematics, Faculty of Engineering, Shinshu University

補完的という概念は1960年代にすでに登場していたが，数学的に補完的部分環の厳密な定義が与えられたのは2000年代に入ってからである．補完的とは，2つの情報があったときに，一方の情報からもう一方の情報についてなにも予測できないということであり，言い換えれば，2つの情報に重複がなく無駄がないということである．

2つの部分環が補完的であることの定義は，部分環から単位限の定数倍を除いた部分が直交することである．本稿では，現在までに知られている補完的部分環の結果と，それに関連する結果について考察する．

1 準備

$\mathcal{A}$を有限次元C^*環とする．すると$\mathcal{A}$は$\oplus_{i=1}^{k} M_{n_i}(\mathbb{C})$と同型になる．$\mathcal{A}$上のトレース（対角成分の和をとるもの）をTrで表す．$\mathcal{A}$は，$A, B \in \mathcal{A}$に対して，

$$\langle A, B \rangle = \mathrm{Tr}(A^* B)$$

とすることで，内積が定義され，ヒルベルト空間になる．

定義 1.1. $\mathcal{A}$の（ユニタル $*$-）部分環$\mathcal{A}_1, \mathcal{A}_2$が補完的であるとは，任意の$A_1 \in \mathcal{A}_1$と$A_2 \in \mathcal{A}_2$で，$\mathrm{Tr}(A_1) = \mathrm{Tr}(A_2) = 0$を満たすものに対して，

$$\mathrm{Tr}(A_1^* A_2) = 0$$

を満たすときをいう．

注意 1.2. $\mathcal{A}_1$と$\mathcal{A}_2$が補完的であることと，$\mathcal{A}_1 \ominus \mathbb{C}I \perp \mathcal{A}_2 \ominus \mathbb{C}I$であることが同値である．また，$E_{\mathcal{A}_1}$と$E_{\mathcal{A}_2}$をそれぞれ$\mathcal{A}_1$，$\mathcal{A}_2$への条件付き期待値とするとき，

$$E_{\mathcal{A}_1} \circ E_{\mathcal{A}_2} = E_{\mathcal{A}_2} \circ E_{\mathcal{A}_1} = \frac{1}{\mathrm{Tr}(I)} \mathrm{Tr}$$

であることも，$\mathcal{A}_1$と$\mathcal{A}_2$が補完的であることと同値である．

本稿では，特に$\mathcal{A} = M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$の場合を考え，$M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$の部分環で，補完的かつ$M_n(\mathbb{C})$と同型なものがいくつ存在するかを考える．

このような問題を考える動機の1つは，状態トモグラフィーと呼ばれる，状態の決定問題にある．まず，ρ を $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ 上の状態（もしくは密度行列）とする．このとき，$M_n(\mathbb{C})$ と同型な部分環の情報から，ρ を決定することを考える．1つ目の部分環から得られる情報は，部分トレース Tr_1 を使って，$\rho_1 = \mathrm{Tr}_1(\rho)$ で与えられる．2つ目の部分環から得られる情報は，同じく部分トレース Tr_2 を使って，$\rho_2 = \mathrm{Tr}_2(\rho)$ である．これら $\rho_1, \rho_2, \ldots$ を使って，ρ を決定したいが，このためにどのような部分環を用いれば，最適な予測ができるかが問題になる．実は，このためにはこれらの部分環が補完的であり，かつ $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ 全体を張る場合が最適となることが知られている．そのため，$M_n(\mathbb{C})$ と同型であり，かつ補完的な部分環で $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ を分割できるかを考える必要がある．

もう1つの動機は，MUB (mutually unbiased bases) との関連性である．ヒルベルト空間 $\mathbb{C}^n$ の正規直交基底（ONB）$\{\phi_i\}$ と $\{\psi_j\}$ は，任意の $1 \leq i, j \leq n$ に対して，

$$|\langle \phi_i, \psi_j \rangle| = \frac{1}{\sqrt{n}}$$

を満たすとき，MUB であるという．ここで，ONB$\{\phi_i\}$ から自然に導かれる可換環を $\mathcal{A}_1$ とする．すなわち，

$$\mathcal{A}_1 = \mathrm{span}\{|\phi_i\rangle\langle\phi_i| : 1 \leq i \leq n\}$$

である．ただし，$x, y, z \in \mathbb{C}^n$ に対して，$|x\rangle\langle y|z = \langle y, z\rangle x$ である．このとき，次の定理がいえる．

定理 1.3. 2つの ONB $\{\phi_i\}$ と $\{\psi_j\}$ が MUB であることと，これらの ONB から自然に導かれる可換環 $\mathcal{A}_1$ と $\mathcal{A}_2$ が補完的であることは同値である．

$\mathbb{C}^n$ の中に MUB がいくつ存在するかという問題は 1980 年代から議論されており，部分的な結果として，n が素数のべき乗の場合 $n+1$ 個の MUB が存在することが知られている．このとき，$n+1$ 個の補完的な部分環によって $M_n(\mathbb{C})$ が張られることも知られている．しかし，n が素数のべき乗でない場合には，MUB の最大個数は知られていない．一番簡単なのは $n = 6$ の場合であるが，この場合でも，最大個数が 3 個であるという予想はあるものの，証明はされていない．補完的な部分環を考察することで，MUB の最大個数を考えるというのが，本研究のもう1つの動機である．

2 補完的部分環

$M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ の中の $M_n(\mathbb{C})$ と同型であり，かつ補完的な部分環を考えてみる．まずは次元を考えてみると，$M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ から $\mathbb{C}I$ を除いた空間の次元は $n^4 - 1$ であり，$M_n(\mathbb{C})$ から $\mathbb{C}I$ を除いた空間の次元は $n^2 - 1$ である．このことから，補完的

な部分環が n^2+1 個存在すれば，それらによって $M_n(\mathbb{C})\otimes M_n(\mathbb{C})$ が張られることがわかる．言い換えれば，$M_n(\mathbb{C})\otimes M_n(\mathbb{C})$ はこれらの補完的な部分環によって分割されることがわかる．

まずは，$n=2$ の場合を考えてみる．$M_2(\mathbb{C})$ のパウリ行列を

$$\sigma_1=\begin{bmatrix}0&1\\1&0\end{bmatrix},\quad \sigma_2=\begin{bmatrix}0&-i\\i&0\end{bmatrix},\quad \sigma_3=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$$

によって定義する．また，$\sigma_0=I$ とおく．このとき，$\{\sigma_i\}_{i=0}^3$ は $M_2(\mathbb{C})$ の直交基底であり，かつ

$$\sigma_1\sigma_2=i\sigma_3,\ \sigma_2\sigma_3=i\sigma_1,\ \sigma_3\sigma_1=i\sigma_2$$

を満たす．これらの性質から，以下の 4 つの部分環は $M_2(\mathbb{C})$ と同型な補完的部分環になる：

$$\begin{aligned}&\mathrm{span}\{I,\sigma_0\otimes\sigma_1,\sigma_1\otimes\sigma_2,\sigma_1\otimes\sigma_3\},\\&\mathrm{span}\{I,\sigma_2\otimes\sigma_1,\sigma_0\otimes\sigma_2,\sigma_2\otimes\sigma_3\},\\&\mathrm{span}\{I,\sigma_3\otimes\sigma_1,\sigma_3\otimes\sigma_2,\sigma_0\otimes\sigma_3\},\\&\mathrm{span}\{I,\sigma_1\otimes\sigma_0,\sigma_2\otimes\sigma_0,\sigma_3\otimes\sigma_0\}.\end{aligned}$$

ここで，5 個の補完的な部分環があれば，$M_2(\mathbb{C})\otimes M_2(\mathbb{C})$ の分割が得られるわけであるが，上記の 4 つに含まれない部分を考えると，

$$\mathrm{span}\{I,\sigma_1\otimes\sigma_1,\sigma_2\otimes\sigma_2,\sigma_3\otimes\sigma_3\}\simeq\mathbb{C}^4.$$

となり，$\mathbb{C}^4$ と同型になってしまう．実際，$n=2$ の場合は，$M_2(\mathbb{C})$ と同型な補完的部分環の最大個数が 4 であることが以下の定理からわかる．

定理 2.1. [5] $\mathcal{A}$ が $M_2(\mathbb{C})$ と同型な $M_2(\mathbb{C})\otimes M_2(\mathbb{C})$ の部分環であり，$M_2(\mathbb{C})\otimes I$ と補完的であれば，

$$\dim(\mathcal{A}\cap I\otimes M_2(\mathbb{C}))\geq 2$$

が成り立つ．

この定理から，直ちに次が導かれる．

定理 2.2. [5] $M_2(\mathbb{C})$ と同型な $M_2(\mathbb{C})\otimes M_2(\mathbb{C})$ の補完的な部分環の最大個数は 4 個である．

MUBや補完的部分環の存在を示す場合には，具体的に構成する証明方法が一般的である．一方で存在しないことを示すのはなかなか難しい．例えば，先に説明した$\mathbb{C}^6$のMUBの最大個数の問題であるが，これを全てパラメータ表示しようと考えると，単純計算で約6^3個の変数が必要になる．ここから，連立方程式を作り，その解が存在しないことを示すことはかなり困難である．そのため，存在しないことを示した定理は意外に少ない．その意味で，この定理は価値のある結果である．

なお，nが2のべき乗の場合には次の定理が知られている．

定理 2.3. [4] nが2のべき乗のとき，$M_2(\mathbb{C})$と同型な$\otimes^k M_2(\mathbb{C})$の補完的部分環が$\frac{4^k-1}{3}-1$個存在する．

ここで，$M_2(\mathbb{C})$と同型な$\otimes^k M_2(\mathbb{C})$の補完的部分環が$\frac{4^k-1}{3}$個存在すれば，$\otimes^k M_2(\mathbb{C})$を分割できるのであるが，$\frac{4^k-1}{3}$個存在するかどうかは，$k=2$の場合を除いて未解決である．

次に，nが2以外の素数の場合を考えよう．この場合も，$M_n(\mathbb{C})$の一般化パウリ行列

$$W=\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & 0 & \dots & 0 \\ 0 & 0 & \lambda^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda^{p-1} \end{bmatrix}, \qquad S=\begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

を使った構成方法を考える．まず，一般化パウリ行列は以下の性質を持つ：

- $S^n=W^n=I$
- $\{S^iW^j\}_{0\le i,j\le p-1}$は$M_n(\mathbb{C})$の直交基底である．
- $SW=\lambda^{-1}WS$
- $S^{k_1}W^{l_1}S^{k_2}W^{k_2}=\lambda^{l_1k_2}S^{k_1+k_2}W^{l_1+l_2}$
- $S^{k_1}W^{l_1}$と$S^{k_2}W^{l_2}$が可換であるための必要十分条件は

$$k_1l_2=k_2l_1 \pmod{p}$$

である．

さらに，次の補題が示せる．

補題 2.4. $S^{i_1}W^{j_1}\otimes S^{k_1}W^{l_1}$と$S^{i_2}W^{j_2}\otimes S^{k_2}W^{l_2}$が可換ではないとき，

$$C^*(S^{i_1}W^{j_1}\otimes S^{k_1}W^{l_1}, S^{i_2}W^{j_2}\otimes S^{k_2}W^{l_2})$$

は$M_n(\mathbb{C})$と同型である．

この補題を用いて，$M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ における一般化パウリ行列の分割を考えると，次の定理が示せる．

定理 2.5. [3] $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ は，n が 2 以外の素数のとき，n^2+1 個の $M_n(\mathbb{C})$ と同型な補完的部分環によって分割される．

また，この定理をさらに一般化し，次の定理を示すことができる．

定理 2.6. [3] $\otimes^{k\ell} M_n(\mathbb{C})$ は，n が 2 以外の素数のべき乗のとき，$\frac{n^{2k\ell}-1}{n^{2k}-1}$ 個の $\otimes^k M_n(\mathbb{C})$ と同型な補完的部分環によって分割される．

最後に本研究に関する参考文献を挙げておく．MUB 問題については [1, 2, 6, 7] に，補完的部分環については [3, 4, 5] に詳しい説明があり，本稿では省略した証明も，これらの論文に載っている．

参考文献

[1] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, F. Vatan, A new proof for the existence of mutually unbiased bases, Algorithmica, **34**, 512-528 (2002).

[2] I. D. Ivanovic, Geometrical description of quantum state determination, J. Phys. A, Math. Gen. **14**, 3241 (1981).

[3] H. Ohno, Quasi-orthogonal subalgebras of matrix algebras, Linear Algebra Appl. **429**, 2146-2158 (2008).

[4] H. Ohno, D. Petz, A. Szántó, Quasi-orthogonal subalgebras of 4×4 matrices, Linear Algebra Appl. **425**, 109-118 (2007).

[5] D. Petz, A. Szántó and M. Weiner, Complementarity and the algebraic structure of four-level quantum systems, J. Infin. Dim. Analysis Quantum Prob., **12**, 1–18 (2009).

[6] P. Wocjan and T. Beth, New construction of mutually unbiased bases in square dimensions, Quantum Inform. compu., **5**, 93-101 (2005).

[7] W. K. Wootters and B. D. Fields, Optimal state determination by mutually unbiased measurements, Ann. Phys., **191**, 363-381 (1989).